PATENT APPLICATION
Attorney Docket: 10003418-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

Applicant:	Engel
Serial No.:	10/005,580
Filed:	11/7/2001
For:	Data Collection Node That Utilizes HTTP Transfer Protocols for Autonomous Data Transfers.
Group Art Unit:	2155
Examiner:	Lazaro, David

CORRECTED BRIEF FOR APPELLANT

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is provided in response to a notice of non-compliance dated 8/10/2007. The sections of the brief filed on June 8, 2007 relating to the arguments have been amended to comply with the notice of non-compliance. This is an appeal from the decision of the Primary Examiner dated 1/12/2007, finally rejecting Claims 4-15 in the above-identified patent application. This brief is filed in response to a Notice of Non-Compliance and corrects the status of the claims and the Summary of the claimed subject matter sections of the brief filed on April 19, 2007.

I. REAL PARTY IN INTEREST

The real party in interest is Agilent Technologies, Inc. having an address as shown below.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Applicant, the Applicant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. STATUS OF THE CLAIMS

Claims 4-15 are currently pending in the above-identified patent application. In the Office Action dated 1/12/2007, the Examiner rejected Claims 4-15 and indicated that the Action was final. Claims 4-15 are the subject of the current appeal. Claims 1-3 have been canceled.

IV. STATUS OF AMENDMENTS

There have been no amendments to the claims since the above-identified final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention is directed to a data collection node and method for using the same to autonomously collect data. With respect to all the Claims, refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application.

With respect to Claim 4, refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application. Claim 4 concerns a data collection node 12, that is configured for remote data collection. The node includes an interface for receiving signals from a sensor 16, an interface for connecting the data collection node to a computer network 14 and a controller 17. The controller generates data based on measurements of the received signals from the sensor and communicates that data to a server 20 using HTTP via the computer network. The controller can receive data from the server that determines the measurements to be made. The controller can also receive commands from a user at a remote location 22, and respond to those commands by altering a measurement that is to be made by the controller.

With respect to Claim 5, refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application and note particularly the paragraph that begins on page 5 at line 5. Claim 5 relates to a data collection node 12, which includes an interface for receiving signals from a sensor 16, an interface for connecting the data collection node to a

computer network 14 and a controller 17. The controller generates data based on measurements of the received signals from the sensor and communicates that data to a server 20 via the computer network. The node also has a proxy server 25. In the situation where a firewall 21 is present between the server 20 and the data collection node 12, the controller 17 communicates with the proxy server so that the firewall does not need to be altered to allow messages to reach the server.

With respect to Claim 6, refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application and note particularly the paragraph that begins on page 4 at line 18 and the paragraph that begins on page 5 at line 5. Claim 6 relates to a data collection node 12, which has an interface that receives signals from a sensor 16, and an interface that connects the node to a computer network 14. A segment of that computer network is part of the Internet. The node also has a controller 17 for generating data based on the received signals and communicating that data to a server 20 on the computer network. The node must also have a clock 13 which can generate time readings that are included with the data that is communicated to the server. Claim 7 depends from Claim 6 and adds the requirement that the clock is set via a message received from server 20, as explained in the paragraph that begins on page 4 at line 29.

Claims 8-15 relate to methods of operating a computer network to collect data. With respect to Claim 8, refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application and note particularly the two-paragraph passage that begins on page 5 at line 19. Claim 8 specifies that the first step of the method consists of providing a data collection node 12 connected to the network 14. The node has an interface for receiving signals from a sensor 16, and a controller 17, which generates data based on measurements of the received signals from the sensor and communicates that data to a server 20 via the computer network. The second step of the method consists of causing the server to provide a Web page for accessing data generated by the controller in response to receiving a registration message from the controller, and of causing the controller to send the generated data to the server after sending that registration message.

Claim 9 requires the basic method of Claim 8 but further specifies that the controller send a registration message to the server **prior** to communicating the generated data to the

server. Claim 10 requires the basic method of Claim 8 but also specifies that the communication of the data be carried out using HTTP. Claim 11 requires the basic method of Claim 8 but adds the requirement that the controller receive commands from a user at a location 22 remote from said node, and responds to those commands by altering a measurement it makes.

Claim 12 requires the basic method of Claim 8 but also specifies that the controller communicates with the server using a proxy server 25 on the network. Please refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application and note particularly the passage beginning on page 5, line 9. Claim 13 requires the basic method of Claim 8 and further specifies the inclusion of a clock 13 to generate time readings that are included with data that is communicated to the server. Please refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application and note particularly the passage beginning on page 4 at line 10. Claim 14 depends from Claim 13 with an additional requirement that the method includes the step of resetting the clock to a time determined by a message received from the server. Please refer to Figure 1 and the discussion thereof that begins on page 3 at line 21 of the present application and note particularly the passage beginning on page 4 at line 29. Claim 15 requires the basic method of Claim 8 with the additional requirement that the web page generated by the server is made accessible via the Internet.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Rejection of Claim 4 under 35 U.S.C. 103(a) as being unpatentable over US 6,405,111 by Rogers, *et al* (hereafter "Rogers") in view of US 6,104,875 by Gallagher, *et al* (hereafter " Gallagher ").

Rejection of Claim 5 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of US 6,920,495 by Fuselier, *et al* (hereafter "Fuselier").

Rejection of Claims 6 and 7 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of US 6,085,243 by Fletcher, *et al* (hereafter "Fletcher").

Rejection of Claims 8-10 and 15 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of US 6,490,617 by Hemphill, *et al* (hereafter "Hemphill").

Rejection of Claim 12 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Hemphill as applied to claim 8 above, and further in view of Fuselier.

Rejection of Claims 13 and 14 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Hemphill as applied to claim 8 above, and further in view of Fletcher.

Rejection of Claim 11 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Hemphill, and further in view of Gallagher.

VI. ARGUMENT

A. Examiner's Burden under 35 U.S.C. 103

To sustain a rejection under 35 U.S.C. 103, the Examiner must show that the combined references teach each of the elements of the claim or that there is some motivation in the art for altering one of the teachings to arrive at the combined set of teachings. "The mere fact that a reference could be modified to produce the patented invention would not make the modification obvious unless it is suggested by the prior art." (*Libbey-Owens-Ford v. BOC Group*, 4 USPQ 2d 1097, 1103). In addition, the Examiner must show that there is some motivation in the art that would cause someone of ordinary skill to combine the references, and that in making the combination, there was a reasonable expectation of success. Where the claimed subject matter has been rejected as obvious in view of a combination of prior art references, a proper analysis under section 103 requires, *inter alia*, consideration of two factors: (1) whether the prior art would have suggested to those of ordinary skill in the art that they should make the claimed composition or device, or carry out the claimed process; and (2) whether the prior art would also have revealed that in so making or carrying out, those of ordinary skill would have a reasonable expectation of success. Both the suggestion and the reasonable expectation of success must be founded in the prior art, not in the applicant's disclosure. *In re Vaeck*, 20 USPQ2d 1438, 1442(CAFC 1991).

B. Rejection of Claim 4 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Gallagher.

Claim 4 is directed to a data node that is configured for remote data collection. The data collection node has an interface that receives signals from a sensor and an interface that connects the node to a computer network. The node must also have a controller for generating data based on the received signals and communicating that data to a server on the computer network via HTTP. The controller must receive data from the server that determines a measurement to be made by the controller and commands from a user at a location remote from the node, the commands altering a measurement made by the controller.

The Examiner states that Rogers teaches all the limitations of the Claim except for the requirement that the controller receive commands from a user at a location remote from the node, said commands altering a measurement made by said controller. The Examiner looks to Gallagher for the missing teachings. The Examiner maintains that it would have been obvious to take the node disclosed by Rogers and modify it as indicated by Gallagher in a way that satisfies the limitations of Claim 4, "as it is desirable to be able to configure a controller after its initial configuration". Applicant submits that the apparatus obtained by combining the teachings of Gallagher with those of Rogers does not satisfy all of the limitations of Claim 4, and that the Examiner's motivation for combining the teachings is also flawed.

Rogers teaches two embodiments of Rogers' invention. The embodiments are shown in Figures 4 and 5. Referring to Figure 4 of Rogers, to satisfy the limitations of Claim 4, the measurement device 210 must correspond to the sensor and the interfaces, and data input controller 200 must correspond to the controller. The node must consist of elements 200, 210, and 230. The network controller 220 is the only device that controller 200 communicates with using HTTP, and hence, must be the server. There is no teaching in this embodiment of receiving commands that alter a data measurement from a user that is remote from the node.

The second embodiment is shown in Figure 5. In this embodiment, the sensors such as sensor 136, communicate directly with server 110 that is accessed by the local shop personnel via browser 100. Hence, the node must consist of the sensors, server 110, and browser 100. Server 110 can communicate with a remote server or browser 120 in this embodiment. Rogers teaches (col. 10, lines 15-28) that the function of controller 200 is now

performed by browser 100, and that network controller 220 has been combined into server 110.

For this second embodiment to satisfy the limitations of Claim 4, there would need to be a second "controller" that receives the signals from the sensors and communicates data based on those signals to server 110. This second controller would need to communicate that data over the network connecting server 110 and the data sensors, and that communication would need to utilize HTTP. Furthermore, that second controller must receive commands from the remote user.

Rogers is silent with respect to any such second controller. At most, Rogers teaches that the sensors communicate with the server over a network using conventional Ethernet protocols (TCP/IP). There is no mention of using HTTP for this purpose. Furthermore, this second controller would need to be in the sensors themselves to satisfy the limitations of Claim 4. Rogers teaches that the sensors are controlled from ActiveX controls in server 110. Hence, if anything, Rogers teaches that the control function is in the server. Accordingly, the embodiment shown in Figure 5 does not satisfy the limitations that the controller receives the signals from the sensors and communicates that data to the server via HTTP.

As noted above, the Examiner admits that Rogers does not teach that controller 200 receives commands from a user at a location remote from the node, the commands altering a measurement made by the controller. The Examiner looks to Gallagher for the missing teachings. Gallagher teaches the programming of a field controller that controls a process by connecting a programming device locally to the computer in the controller and downloading new code into the microprocessor. The Examiner interprets the downloading of the new code as a command that alters a measurement made by the microprocessor. However, it should be pointed out that Gallagher does not teach that the new code alters any measurements made by the local microprocessor with respect to the sensors attached thereto. Gallagher refers to changes in algorithms used to process the collected data to provide a new control function for the node.

The Examiner suggests that it would be obvious to modify the teachings of Rogers to include downloading of code to controller 200 because it would allow the initial

configuration of the controller to be changed in the field. It should be noted that Rogers already teaches the downloading of code to controller 200 from network controller 220 in response to commands from a user at the local controller 200. Hence, the new functionality suggested by the Examiner is already in the system of Rogers. Accordingly, the Examiner's motivation to make the alteration is flawed.

The issue here is whether the commands would be sent from a user at a remote location to controller 200. Gallagher teaches that the controllers are reprogrammed from a device that is connected directly to each process computer. Rogers teaches that a user at controller 200, which is a general purpose computer, specifies the tests to be run and at least part of the data needed to run the test is downloaded via the network controller. Rogers also teaches that the server on which the data is stored can be connected to a remote browser. Hence, at best, the combination of Gallagher and Rogers teaches altering the programs on server 110 shown in Figure 5 from the remote browser 120. However, as noted above, this embodiment fails to teach the other limitations of Claim 4. The Examiner has not pointed to any teaching that input controller 200 taught in Figure 4 would receive commands from a remote user.

Hence, Applicant submits that there would be no reason to make the combination of prior art suggested by the Examiner to improve the system taught by the primary reference. And, furthermore, such a combination would not satisfy all of the limitations of Claim 4. Accordingly, Applicant submits that the Examiner has failed to make a *prima facie* case for obviousness with respect to Claim 4.

C. Rejection of Claim 5 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Fuselier.

Claim 5 is directed to a data node which has an interface that receives signals from a sensor and an interface that connects the node to a computer network. The node also has a controller for generating data based on the received signals and communicating that data to a server on the computer network. The controller communicates with the server via a proxy server, so that in the situation where a firewall is present between the server and the data collection node, the firewall does not need to be altered to allow messages to reach the server.

The Examiner states that Rogers teaches all the limitations of the Claim except for the limitation that the controller communicates with a server via a proxy server on the computer network. The Examiner looks to Fuselier for the missing teachings. The Examiner maintains that it would have been obvious to take the data collection node disclosed by Rogers and modify it as indicated by Fuselier to incorporate a proxy server on the computer network "as it is desirable to prevent unauthorized access to a server while not prohibiting valid messages". Applicant submits that the Examiner's motivation for combining the teachings is flawed.

The issue here is not whether a proxy server offers a useful means for preventing unauthorized access to a server while permitting legitimate access. The issue here is whether adding a proxy server to the system taught by Rogers would offer that system any significant advantage that would cause someone of ordinary skill to increase the complexity of the system taught in Rogers. Rogers teaches a system for which the users, the technicians at a set of automotive workshops, are already known. In some cases, the shops are required to pay for the services offered by the server, and hence, the user must subscribe to the server. In systems in which the users are all known, a proxy server does not provide any benefit beyond that provided by the access control system already on the server. Typically, a password and conventional data encryption is sufficient.

Proxy servers provide a means for validating a user that is not already known to the server without having to alter the server. The proxy server is, in essence, a known user of the server. An unknown user of the system directs its messages to the proxy server, which provides the validation of the unknown user. If the unknown user is validated, the message is communicated to the server. Since the system taught in Rodger's already knows its users, the proxy server validation is not needed. The present invention, in contrast, is directed to a system in which unknown users may be given some form of access to the collection nodes, and hence, a proxy server provides an advantage.

Hence, Applicant submits that there would be no reason to make the combination of prior art that the Examiner suggests would improve the system taught by Rogers, the primary

reference. Accordingly, Applicant submits that the Examiner has failed to make a *prima facie* case for obviousness with respect to Claim 5.

D. Rejection of Claims 6 and 7 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Fletcher

Claim 6 is directed to a data node that is configured for remote data collection. The data collection node has an interface that receives signals from a sensor and an interface that connects the node to a computer network. A segment of that computer network is part of the Internet. The node must also have a controller for generating data based on the received signals and communicating that data to a server on the computer network. The node must also have a clock which can generate time readings that are included with the data that is communicated to the server. Claim 7 depends from Claim 6 and adds the requirement that the clock is set via a message received from the server.

With respect to Claim 6, the Examiner states that Rogers teaches all the limitations of the Claim except for the inclusion of a clock for generating time readings that are included with the data communicated to the server. The Examiner looks to Fletcher for the missing teachings. The Examiner maintains that it would have been obvious to take the data collection node disclosed by Rogers and modify it as indicated by Fletcher to include a clock generating time stamps "as it is desirable to have properly ordered and meaningful data". Applicant submits that the Examiner's motivation for combining the teachings is flawed.

Applicant submits that Rogers teaches sending data to the server for processing the data, but does not teach that the server stores the data after the server processes the data. Hence, Applicant submits that there is no reason to provide a clock and time stamp on the data. The Examiner asserts that Rogers does describe (in col. 11, lines 10-67) a situation in which a history of collected data is accessed, that the data is stored related to the collected measurements, and hence, the Examiner argues that the addition of time stamps would be beneficial. Applicant respectfully disagrees with the Examiner's reading of Rogers.

The passage in Rogers to which the Examiner points (column 11, lines 10-67) does not concern the storage of measurement data collected at the node, but of vehicle

specifications, inventory levels, and other financial and operational details relevant to business operation. The Examiner has not pointed to any teaching regarding the storage or retrieval of the measurement data, and hence, Applicant maintains that the system of Rogers would not benefit from the addition of a clock that generates time stamps on the measurement data communicated to the server. Furthermore, Applicant submits that the servers taught in Rogers are general purpose computers that have their own clocks, and hence, can provide time stamps corresponding to the time the data is received. Such server time stamps already provide the benefits suggested by the Examiner without the cost of duplicating the clocks at the service nodes and assuring that all of the clocks are synchronized.

The clocks provide an advantage in the present invention because the present invention allows the nodes to collect a number of different sets of data from the sensors before relaying those measurements to the server. Hence, the clock at the server is needed as part of the data sensors. In addition, the present invention anticipates situations in which data from a plurality of nodes must be combined, and hence, the time stamps are needed to properly combine the data.

Accordingly, Applicant submits that the Examiner has failed to make a *prima facie* case for obviousness with respect to Claim 6 and the Claims dependent therefrom.

Claim 7 depends from Claim 6 and further requires that the clock is set via a message received from the server. The Examiner looks to Fletcher for that specific teaching.

First, Applicant repeats the argument presented above with respect to Claim 6 regarding the lack of motivation to provide a clock.

Second, Applicant submits that there would be no reason, even if a clock were provided at the local automotive shop site and used to time stamp data sent from that shop, for the clock to be reset according to a remote server. Such centralized synchronization is relevant for a system in which multiple measurements must be coordinated with one another; however, Rodgers does not teach such a system. Rogers teaches a system in which the measurement data communication between a single user and the server is separate from and irrelevant to the measurement data communication between another user at a different

location and that same server. Hence, discrepancies in clock timings among those users would not be important, and there would be no need for a server-originated reset which adds cost and complexity to the system.

Accordingly, there are additional reasons for allowing Claim 7.

E. Rejection of Claims 8-10 and 15 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Hemphill.

These claims relate to methods of operating a computer network to collect data.

In the method specified by Claim 8, from which the other Claims depend, a data collection node connected to a network is provided. The node has an interface for receiving signals from a sensor and a controller, which generates data based on measurements of the received signals from the sensor and communicates that data to a server via the computer network. The server provides a Web page for accessing data generated by the controller in response to receiving a registration message from the controller. The controller sends the generated data to the server after sending that registration message.

With respect to Claim 8, the Examiner states that Rogers teaches all the limitations of the Claim except for two requirements. The first is that the server provides a web page for accessing data generated by the controller in response to receiving a registration message from the controller, and the second is that the controller sends a message to the server containing data generated by the controller after the controller sends the registration message. The Examiner looks to Hemphill for the missing teachings. The Examiner maintains that it would have been obvious to take the method disclosed by Rogers and modify it as indicated by Hemphill in a way that satisfies the claim limitations "as it is desirable to provide information about devices at the time of discovery (Hemphill, col. 1, lines 52-59)." Applicant submits that the apparatus obtained by combining the teachings of Hemphill with those of Rogers does not satisfy all of the limitations of Claim 8.

Claim 8 requires the provision of a web page for accessing data generated by the controller, that data being based on measurements of signals received from the sensor. The

Examiner states that Hemphill teaches (col. 5, lines 3-29 and col. 5, line 64 – col. 6, line 12) that after management of the device begins in response to the registration message, the information from the node can be sent to the server and is further available through a web page. Applicant submits that the passages cited relate to the communication of management data, such as device address and status, not to any measurement data based on signals received from a sensor within the node. Indeed, the text of column 5 lines 64-67 makes it clear that the remote browser is present simply for "accessing and displaying **management information** from the management server" and any of the web-enabled devices. There is no teaching the information contains any data collected from a sensor.

Furthermore, the passage in Hemphill (col. 1, lines 52-59), cited by the Examiner to provide motivation for modifying the system of Rogers with the teachings of Hemphill, also makes it very clear that the information communicated to the web page relates to network management, which is simplified if the devices connected to the network self-identify. The "information about devices at the time of discovery" mentioned therein is not the same as information based on measurements of signals received from sensors as required by Claim 8.

At most, the combination of Rodgers and Hemphill teaches a system in which the service node sends a message to the server specifying the configuration at the server node in a registration message and that configuration information is displayed on a web page that that can be accessed by a browser connected to the server. The Examiner has not pointed to any teaching in Rodgers or Hemphill that the web page in question would provide access to the data collected by sensors at the service node. In this regard, it should be noted that Hemphill does not teach that the remote nodes provide any information other than that needed to "self-describe" the node. There is no teaching that the web page will allow someone to have access to the ongoing data streams within the nodes in question. Hence, Applicant submits that the Examiner has failed to make a *prima facie* case for obviousness with respect to Claim 8 and the Claims dependent therefrom.

F. Rejection of Claim 12 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Hemphill as applied to Claim 8 above, and further in view of Fuselier.

Claim 12 depends from Claim 8, and further requires that the controller communicates with the server using a proxy server on the network.

The Examiner states that Rogers in view of Hemphill teaches all the limitations of Claim 8 except for requiring that the controller communicates with the server via a proxy server on the computer network. The Examiner looks to Fuselier for the missing teachings. The Examiner maintains that it would have been obvious to take the method disclosed by Rogers in view of Hemphill and modify it as indicated by Fuselier "as it is desirable to prevent unauthorized access to a server while not prohibiting valid messages". Applicant submits that the method obtained by combining the teachings of Fuselier with those of Rogers and Hemphill does not satisfy all of the limitations of Claim 12, and that the Examiner's motivation for combining the teachings is also flawed.

First, as noted above with respect to Claim 8, the combination of Rogers and Hemphill does not teach the limitation regarding web page access to measurement data generated by the controller. Fuselier does not provide the missing teachings. Second, as noted above with respect to Claim 5, there would be no motivation to combine the teachings of Rogers and Fuselier in a way that would satisfy the proxy server limitation contained in Claim 12. Hemphill does not provide the missing motivation. Hence, Applicant submits that the Examiner has failed to make a *prima facie* case for obviousness with respect to Claim 12.

G. Rejection of Claims 13 and 14 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Hemphill as applied to Claim 8 above, and further in view of Fletcher.

Claim 13 depends from Claim 8, and further requires the inclusion of a clock to generate time readings that are included with data that is communicated to the server. Claim 14 depends from Claim 13 with the additional requirement that the method includes the step of resetting the clock to a time determined by a message received from the server.

The Examiner states that Rogers in view of Hemphill teaches all the limitations of Claims 13 and 14 except those relating to the clock. The Examiner looks to Fletcher for the missing teachings. The Examiner maintains that it would have been obvious to take the

method disclosed by Rogers in view of Hemphill and modify it as indicated by Fletcher in a way that satisfies the limitations of Claims 13 and 14 "as it is desirable to have properly ordered and meaningful data". Applicant submits that the method obtained by combining the teachings of Fletcher with those of Rogers and Hemphill does not satisfy all of the limitations of Claims 13 and 14, and that the Examiner's motivation for combining the teachings is also flawed.

First, as noted above with respect to Claim 8, the combination of Rogers and Hemphill does not teach the limitation regarding web page access to measurement data generated by the controller. Fletcher does not provide the missing teachings. Second, as noted above with respect to Claims 6 and 7, there would be no motivation to combine the teachings of Rogers and Fletcher in a way that would satisfy the clock limitations contained in Claims 13 and 14. Hemphill does not provide the missing motivation. Hence, Applicant submits that the Examiner has failed to make a *prima facie* case for obviousness with respect to Claims 13 and 14.

H. Rejection of Claim 11 under 35 U.S.C. 103(a) as being unpatentable over Rogers in view of Hemphill, and further in view of Gallager.

Claim 11 is dependent from Claim 8 and includes a further limitation that the controller receives data from the server that determines a measurement made by the controller and commands from a user at a location remote from the node, the commands altering a measurement made by the controller. Applicant repeats the arguments made above with respect to the lack of obviousness with respect to Claim 8 in view of Rogers and Hemphill. Gallager does not provide the missing teachings.

The Examiner looks to Gallagher for the additional limitation to the invention of Claim 8 that is found in Claim 11. Gallagher teaches the programming of a field controller that controls a process by connecting a programming device locally to the computer in the controller and downloading new code into the microprocessor. The Examiner interprets the downloading of the new code as a command that alters a measurement made by the microprocessor. However, it should be pointed out that Gallagher does not teach that the new

code alters any measurements made by the local microprocessor with respect to the sensors attached thereto. Gallagher refers to changes in algorithms used to process the collected data to provide a new control function for the node.

The Examiner suggests that it would be obvious to modify the teachings of Rogers to include downloading of code to controller 200 because it would allow the initial configuration of the controller to be changed in the field. It should be noted that Rogers already teaches the downloading of code to controller 200 from network controller 220 in response to commands from a user at the local controller 200. Hence, the new functionality suggested by the Examiner is already in the system of Rogers. Accordingly, the Examiner's motivation to make the alteration is flawed.

It should be noted that Gallagher does not teach sending commands from a user at a remote location to controller 200. Gallagher teaches that the controllers are reprogrammed from a device that is connected directly to each process computer: Rogers teaches that a user at controller 200, which is a general purpose computer, specifies the tests to be run and at least part of the data needed to run the test is downloaded via the network controller. Rogers also teaches that the server on which the data is stored can be connected to a remote browser. Hence, at best, the combination of Gallagher and Rogers teaches altering the programs on server 110 shown in Figure 5 from the remote browser 120. However, as noted above, this embodiment fails to teach the other limitations of Claim 8. The Examiner has not pointed to any teaching that input controller 200 taught in Figure 4 would receive commands from a remote user.

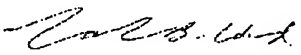
Hence, Applicant submits that there would be no reason to make the combination of prior art suggested by the Examiner to improve the system taught by the primary reference. And, furthermore, such a combination would not satisfy all of the limitations of Claim 11. Accordingly, Applicant submits that the Examiner has failed to make a *prima facie* case for obviousness with respect to Claim 11.

VII. CONCLUSION

Applicant respectfully submits that for the reasons of fact and law argued herein, the decision of the Examiner in finally rejecting Claims 4-15 should be reversed.

I hereby certify that this paper (along with any others attached hereto) is being sent via facsimile to fax number: 571-273-8300. This paper is filed in triplicate.

Respectfully Submitted,



Calvin B. Ward
Registration No. 30,896
Date: September 4, 2007

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925)855-9214

APPENDIX

THE CLAIMS ON APPEAL:

4. A data collection node comprising:

an interface for receiving signals from a sensor;

an interface for connecting said data collection node to a computer network; and

a controller for generating data based on measurements of said received signals and communicating that data to a server via said computer network,

wherein said controller communicates said data via HTTP and

wherein said controller receives data from said server that determines a measurement to be made by said controller and commands from a user at a location remote from said node, said commands altering a measurement made by said controller.

5. A data collection node located at a first location comprising:

an interface for receiving signals from a sensor;

an interface for connecting said data collection node to a computer network; and

a controller for generating data based on measurements of said received signals and communicating that data to a server via said computer network,

wherein said controller communicates with said server via a proxy server on said computer network.

6. A data collection node comprising:

an interface for receiving signals from a sensor;

an interface for connecting said data collection node to a computer network having a segment that is part of the Internet;

a controller for generating data based on measurements of said received signals and communicating that data to a server via said computer network; and

a clock for generating time readings that are included with data that is communicated to said server.

7. The data collection node of Claim 6 wherein said clock is set via a message received from said server.

8. A method for operating a computer network to collect data, said method comprising the steps of:

providing a data collection node connected to said network, said data collection node comprising:

an interface for receiving signals from a sensor; and

a controller for generating data based on measurements of said received signals and communicating that data to a server via said computer network;

causing said server to provide a web page for accessing data generated by said controller in response to receiving a registration message from said controller; and

causing said controller to send a message to said server containing data generated by said controller after said controller sends said registration message.

9. The method of Claim 8 further comprising the step of causing said controller to send a registration message to said server prior to communicating said data to said server.

10. The method of Claim 8 wherein said controller communicates said message containing said data via HTTP.

11. The method of Claim 8 wherein said controller receives data from said server that determines a measurement made by said controller and commands from a user at a location remote from said node, said commands altering a measurement made by said controller.

12. The method of Claim 8 wherein said controller communicates with said server via a proxy server on said computer network.

13. The method of Claim 8 wherein said data collection node further comprises a clock for generating time readings that are included with data that is communicated to said server.

14. The method of Claim 13 further comprising the step of resetting said clock to a time determined by a message received from said server.

15. The method of Claim 8 further comprising the step of providing access to said Web page via the Internet.

Evidence Appendix

none

Related Proceedings Appendix

none